10/26/00

A

Attorney Docket No.: SONY-50P4042.US.P

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

I hereby certify that this transmittal of the below described documents is being deposited with the United States Postal Service in an envelope bearing Express Mail Postage and an Express Mail label, with the below serial number, addressed to the Commissioner of Patents and Trademarks, Washington, D.C., 20231, on the below date of deposit.

Express Mail Label No.:	EL676375163US	Name of Person Making the Deposit:	ANTHONY CHOU
Date of Deposit:	10/24/00	Signature of the Person Making the Deposit:	Anthony Chou

Inventor(s): Ryuichi Iwamura

Title: METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER

The Commissioner of Patents and Trademarks
Washington, D.C. 20231
Sir:

Transmittal of a Patent Application
(Under 37 CFR §1.53)

Transmitted herewith is the above identified patent application, including:

- X Specification, claims and abstract, totaling 31 pages.
- ____ Formal drawings, totaling ____ pages.
- X Informal drawings, totaling 9 pages.
- X Declaration and Power of Attorney.
- ____ Information Disclosure statement.
- ____ Form 1449
- X Assignment(s)
- X Assignment Recordation Form (duplicate)
- ____ Preliminary Amendment

FEES DUE

The fees due for filing the specification pursuant to 37 C.F.R. § 1.16 and for recording of the Assignment, if any, are determined as follows:

CLAIMS					
	NO. OF CLAIMS		EXTRA CLAIMS	RATE	FEES
Basic Application Fee					$710.00
Total Claims	25	Minus 20=	5	X $18 =	$90.00
Independent Claims	3	Minus 3=	0	X $80=	$0.00
If multiple dependent claims are presented, add $260.00					$0.00
Add Assignment Recording Fee of $40.00 If Assignment document is enclosed					$40.00
TOTAL APPLICATION FEE DUE					$840.00

PAYMENT OF FEES

The full fee due in connection with this communication is provided as follows:

1. Not enclosed

   [ ] No filing fee is to be paid at this time.

2. Enclosed

   [X] Filing fee

   [X] Recording assignment

   [ ] Petition fee for filing by other than all the inventors or person on behalf of the inventor where inventor refused to sign or cannot be reached

   [ ] For processing an application with specification in a non-English language

   [ ] Processing and retention fee

   [ ] Fee for international-type search report

   [X] The Commissioner is hereby authorized to charge any additional fees associated with this communication or credit any overpayment to Deposit Account No.: 23-0085. A duplicate copy of this authorization is enclosed.

   [X] A check in the amount of $840.00

   [ ] Charge any fees required or credit any overpayments associated with this filing to Deposit Account No.: 23-0085.

This application is filed pursuant to 37 C.F.R. § 1.53 in the name of the above-identified Inventor(s).

Please direct all correspondence concerning the above-identified application to the following address:

WAGNER, MURABITO & HAO LLP
Two North Market Street, Third Floor
San Jose, California 95113
(408) 938-9060

[X] This transmittal ends with this page.

Respectfully submitted,

Date: 10/24/2000

By: Ronald M. Pomerenke
Ronald M. Pomerenke
Reg. No. 43,009

SONY 50P4042 US P

UNITED STATES PATENT APPLICATION FOR

METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER

Inventor:

Ryuichi Iwamura

Prepared by:

WAGNER, MURABITO & HAO LLP

TWO NORTH MARKET STREET

THIRD FLOOR

SAN JOSE, CALIFORNIA 95113

(408) 938-9060

METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER

FIELD OF THE INVENTION

The present invention relates to the field of digital signal processing. Specifically, the present invention relates to a system and method for securely decoding an encrypted digital signal.

BACKGROUND ART

The field of digital video signal processing has seen rapid development in recent years. For example, digital broadcasting is now beginning to replace analog broadcasting. Digital broadcasting must be securely protected, as digital broadcast data can easily be copied without degrading the quality of the content. Currently, most digital broadcast streams are encrypted, for example, with Data Encryption Standard (DES). When using DES, the broadcast service provider provides a Smartcard to each subscriber. The Smartcard is inserted in a set-top box, which communicates with the Smartcard to generate an encryption key. The key is sent to a decryptor, which decrypts the encrypted stream with the key. The key is renewed frequently, for example every five seconds.

A conventional digital cable set-top box 130 for decrypting and decoding a digital signal is illustrated in Figure 1. When playing a signal which is currently being received, front-end 150 tunes to a digital cable signal, demodulates and sends the signal to broadcast decryptor 152. The bitstream decrypted by broadcast decryptor 152 is sent to transport parser/de-multiplexer 162 through switch 155. In this mode, switch 155 connects broadcast decryptor 152 in chip A

180 to transport parser/de-multiplexer 162 in chip B 190. Thus, unfortunately, the decrypted signal is exposed ("in the clear") on a pin of chip A 180 and chip B 190. Therefore, in this conventional system, the decrypted bitstream is vulnerable to being stolen, copied, and distributed without the copyright-holder's consent.

After chip B 190 receives the signal, transport parser/de-multiplexer 162 parses and de-multiplexes the decrypted bitstream. Then, it sends video packets to video decoder 170 and audio decoder 172, respectively. Video decoder 170 decodes the video data and sends the decoded signal to a television set 174. Similarly, audio decoder 172 decodes the audio data and sends the decoded signal to television set 174.

Chip A 180 contains necessary circuitry for protecting the signal when it is transported for storage. In the recording mode, the decrypted bitstream from broadcast decryptor 152 is re-encrypted in Digital Transmission Content Protection (DTCP) block 154. DTCP is the encryption for the IEEE 1394 serial bus. The re-encrypted bitstream is sent to hard disk drive (HDD) 158 via the IEEE 1394 bus 176.

When playing back the recorded signal, the bitstream is transferred from HDD 158 though the IEEE 1394 interface 156 to the DTCP block 154, where the signal is decrypted. The decrypted signal is sent to transport parser/de-multiplexer 162 and decoded as described above. Thus, while the signal is encrypted while on the IEEE 1394 bus, unfortunately, it is not encrypted (e.g., it is in the clear) while

being transferred between chip A 180 and chip B 190. Again, the un-encrypted bitstream is vulnerable to theft when it is transferred between the two chips.

The received bitstream contains encryption information. Transport parser/de-multiplexer 162 extracts encryption key data from the decrypted bitstream and sends it to the host CPU 114 though bus interface 164 via PCI bus 115. The host CPU 114 communicates with the Smartcard 113 through Smartcard interface 110 to generate the encryption keys. The Smartcard 113 is a 'black box,' for example, the internal signal process is kept secret.

The host CPU 114 sends the keys to the broadcast decryptor 152 over the PCI bus 115. The broadcast decryptor 152, in turn, uses the keys to decrypt the incoming stream. Because the keys are frequently renewed, the host CPU 114 must generate and send a new key to the broadcast decryptor 152 within the time period specified in the requirements. When an even key is currently being used by the broadcast decryptor 152, a new odd key is sent to broadcast decryptor 152. The broadcast decryptor 152 has an even and an odd key register.

The received bitstream also contains encryption information that is used by the decryptor directly. For example, the Motion Pictures Expert Group 2 (MPEG-2) packet header contains transport scrambling control (TSC) bits. The TSC bits tell whether the packet is encrypted and whether the encryption key was even or odd. Based on the TSC bits, the broadcast decryptor 152 selects either the even or the odd key to decrypt the packet. After decryption, the TSC bits in the header are reset to 'un-encrypted.'

Unfortunately, this conventional system exposes the encryption key on the PCI bus 115 when the CPU 114 transfers the key to the decryptor 152. Consequently, it is possible to steal the key by monitoring the PCI bus 115. If a series of keys are stolen, it is possible to determine the actual key generation mechanism. Once the key generation mechanism is known, access to programs for which a fee is charged is no longer secure. Even if the key generation mechanism is not determined, the stolen keys can be sent over a network to other set-top boxes, thus defeating the encryption.

SUMMARY OF THE INVENTION

Therefore, it would be advantageous to provide a method and system providing for a secure digital signal decryptor and decoder. A further need exists for a method and/or system which decrypts and decodes a signal without exposing a decrypted signal on the pins of a integrated circuit when the signal is transferred between two integrated circuits. A still further need exists for such a system which does not expose an encryption key on a communication link.

The present invention provides a method and system providing for a secure digital signal decryptor. Embodiments provides a method and system which decrypt and decode a signal without exposing the decrypted signal on the pins of an integrated circuit. Embodiments provide a method and system which decrypt and decode a signal without exposing an encryption key on a communication bus. The present invention provides these advantages and others not specifically mentioned above but described in the sections to follow.

A method and system for securely decrypting and decoding a digital signal is disclosed. One embodiment of the present invention first receives an encrypted signal at a first logical circuit. Next, this embodiment determines a broadcast encryption key for the encrypted signal at a first location separate from the first logical circuit. For example, the separate location where the broadcast key was determined may be across a communication link from the first circuit where the signal is being received. Then, the broadcast encryption key is encrypted and transferred over the communication link. Next, at the first logical circuit, the encrypted broadcast encryption key is decrypted. Therefore, the broadcast

encryption key is determined. Then, at said first logical circuit, the encrypted signal is decrypted using the broadcast encryption key. Consequently, the encrypted signal is decrypted without exposing the broadcast encryption key on the communication link in an un-encrypted form, for example, without exposing the un-encrypted signal in the clear.

Another embodiment of the present invention, in addition to the steps in the above paragraph, accesses a value in a hidden register on the first logical circuit. Using this value, the broadcast encryption key is encrypted. The first circuit may then use the value in its hidden register to decrypt the broadcast key when it receives it. In still another embodiment, the hidden register may be written to.

In yet another embodiment, a value is stored in a hidden register on the first logical circuit, for example, at manufacture time. This value is provided to a host computer system, which uses the value for encryption purposes.

In another embodiment, at least one of a plurality of hidden registers on the first logical circuit is selected to be used to encrypt the broadcast encryption key. Then, the selected register(s) are indicated to the first logical circuit.

In one embodiment, a value in non-volatile memory on the first logical circuit is accessed. Using this value, an encryption key is encrypted. In one embodiment, the non-volatile memory contains user-dependent data.

Yet another embodiment provides a method which first generates a local encryption key. Then, the local encryption key is transferred across a communication link to a first logical circuit and to a second logical circuit. With the local encryption key, a digital signal at the first logical circuit is encrypted. This encrypted signal is transferred to the second logical circuit. Thus, the signal is not exposed in an un-encrypted form. Next, the second logical circuit uses the local encryption key to decrypt the signal.

In another embodiment, the host processor accesses a value in a register on the first circuit, which it uses to encrypt the local encryption key before it is transferred across the communication link to the first circuit. In a similar fashion, the host process access a register on the second circuit, which is used to encrypt the local key before it is sent to the second circuit. The first and second circuits use the values in their respective hidden registers to decrypt the local keys.

In yet another embodiment, in addition to the steps in the above paragraph, a command is issued to the first logical circuit to modify a header in the signal bitstream to indicate that the bitstream is encrypted. Furthermore, the command may indicate the type of encryption key, for example, odd or even.

A still another embodiment provides for a system for processing a digital signal. The system comprises a first logical circuit comprising a first hidden register and a local encryptor. The first logical circuit is operable to decrypt a first local key using a first value stored in the first register. The system also comprises a second logical circuit which, in turn, comprises a local decryptor and a second

hidden register. The second logical circuit is operable to decrypt a second local key using a second value stored in the second register. Furthermore, the local decryptor is operable to decrypt a signal encrypted with the local encryptor. Thus, the system is able to decrypt the received broadcast signal without exposing an un-encrypted encryption key and without exposing an un-encrypted broadcast signal.

Another embodiment adds a host processor and memory to this system. A communication link connects the host processor to the first logical circuit and to the second logical circuit. The memory contains instructions, which when run on the host processor, are operable to access the first hidden register and generate the first local key and to access the second hidden register and generate the second local key.

In still another embodiment, the first logical circuit further comprises a plurality of hidden registers and a control register operable to store a value to indicate which of the hidden registers is used for encryption purposes.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an illustration of a conventional digital bitstream decryptor and decoder.

Figure 2 is an illustration of an exemplary digital bitstream decryptor and decoder, according to an embodiment of the present invention.

Figure 3a is an illustration of a local encryptor, according to an embodiment of the present invention.

Figure 3b is an illustration of a local decryptor, according to an embodiment of the present invention.

Figure 4 is a flowchart illustrated the steps of a process of securely transferring an encryption key across a communication link, according to an embodiment of the present invention.

Figure 5 is a flowchart illustrated the steps of a process of securely transferring an bitstream between logical circuits, according to an embodiment of the present invention.

Figure 6 is a schematic of a computer system, which may be used to implement embodiments of the present invention.

Figure 7 is a schematic illustration of a local encryptor with multiple hidden registers and a control register, according to an embodiment of the present invention.

Figure 8 is an illustration of an exemplary digital bitstream decryptor and decoder with non-volatile memory, according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of the present invention, a method and system for securely decrypting and decoding a digital signal, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be recognized by one skilled in the art that the present invention may be practiced without these specific details or with equivalents thereof. In other instances, well known methods, procedures, components, and circuits have not been described in detail as not to unnecessarily obscure aspects of the present invention.

NOTATION AND NOMENCLATURE

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits that can be performed on computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer executed step, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as “indexing” or "processing" or "computing" or "translating" or "calculating" or "determining" or “scrolling” or "displaying" or “recognizing” or “generating” or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER

The present invention provides for a method and system for securely decrypting and decoding a digital signal. In order to combat theft of encryption keys on a communication link, embodiments of the present invention encrypt the key itself before transferring it across a bus. Additionally, embodiments also provide for a local encryption key so that the bitstream is not exposed un-encrypted on the pins of an integrated circuit.

Figure 2 illustrates a diagram of an exemplary digital decoder 200. The decoder 200 comprises a first logical circuit 203 and a second logical circuit 204. The logical circuits may be, for example, separate integrated circuits. Additionally,

the system comprises a hard disk drive 217, which may be used for storing (recording) digital signals. These signal may be transferred over the IEEE 1394 bus 216 in an encrypted form.

The first logical circuit 203 comprises a broadcast encryptor 202, a local encryptor 220, a Digital Transmission Content Protection (DTCP) block 223, and a switch 205 connecting local encryptor 220 to either the DTCP block 223 or the broadcast decryptor 202. The broadcast decryptor 202, local encryptor 220, and local decryptor 221 have hidden registers 310c, 310a, and 310b respectively.

The second logical circuit 204 comprises a local decryptor 221, a transport parser/de-multiplexer 207 which parses and de-multiplexes the decrypted bitstream. Additionally, this circuit 204 has a video decoder 208 and audio decoder 209. Finally, the circuit has interfaces such as Smartcard interface 210 and bus interfaces 206 and 211.

Bus interfaces 206 and 211 may be any of a variety of physical bus interfaces, including but not limited to a Universal Serial Bus (USB) interface, Personal Computer (PC) Card interface, CardBus or Peripheral Component Interconnect (PCI) interface, mini-PCI interface, Personal Computer Memory Card International Association (PCMCIA) interface, Industry Standard Architecture (ISA) interface, or RS-232 interface.

The system also comprises a host computer system 214, which may be a computer system such as illustrated in Figure 6. The host computer system 214 is

separate from the first 203 and second 204 circuits in that a communication link 215 or other mechanism separates them. For security, embodiments of the present invention will encrypt keys transferred between the host computer 214 and the circuits (203, 204). In a preferred embodiment, communication link 215 is a PCI bus.

Referring now to Figure 3a, the local encryptor 220 will be discussed in more detail. The local encryptor 220 inputs an un-encrypted bitstream 314 from another part of the first logical circuit 203. The local encryptor 220 outputs an encrypted bitstream 342, which may be input to the local decryptor 221. The local encryptor 220 also may communicate with the host processor 214 via the communication link 215. The local encryptor 220 comprises an even key register 302a and an odd key register 304a, which may be used for storing even and odd encryption keys, respectively.

The hidden register 310a is used to store a value which, in one embodiment, the host computer system 214 may access and use to encrypt keys before transferring them across a communication link 215. After transfer, the same value is used by the first circuit 203 to decrypt the key. The value may be stored in the hidden register 310a when the circuit 203 is manufactured. The present invention provides considerable flexibility regarding the hidden registers 310. In one embodiment, a software engineer, who knows the value stored in the hidden registers 310, provides this information to the host computer system 214. In this fashion, the host system 214 does not need to access the hidden registers 310.

Thus, the connection between the hidden register 310a and the communication link 215 is optional.

In one embodiment, the hidden register 310a is non-volatile. In one embodiment, the host computer 214 may write to the hidden registers 310. In one embodiment, the hidden register 310a is 64 bits. However, the present invention is well-suited to hidden registers 310 of other sizes, as it may be useful, although it is not required, for the hidden register 310a to be the same size as the broadcast key.

The encryptor 220 also contains key decryption logic 312a, which uses the value in the hidden register 310a along with knowledge of the process used to encrypt the key to decrypt it. For example, if the key was encrypted by performing an exclusive OR with the key and the value from the hidden register 310a, then the key decrypt logic 310a performs an exclusive OR on the encrypted key with the value from the hidden register 310a to obtain the original un-encrypted key. The present invention is well-suited to other methods of encrypting/decrypting the key while using the value from the hidden register 310a.

Still referring to Figure 3a, the local encryptor 220 also has bitstream encrypting logic 306. This logic 306 make use of the key passed to it from the host computer system 214. Finally, the local encryptor 220 has a Transport Scrambling Control (TSC) register 308. This register 308 may be written to by the host computer system 214 to direct the encryptor 220 to modify the TSC bits in the header of the signal bitstream to indicate that the bitstream is encrypted and

whether the encryption is odd or even. For example, the transport scrambling control bits in the transport packet may be set to "10" for an even key and "11" for an odd key. The bits may also be set to "01" to indicate the bitstream is not scrambled. The present invention is not, however, limited to using the values with the control register 308 in this fashion. The value in the TSC register 308 may also be used to determine which key register (302a, 304a) should be selected by encryptor switch 303.

Referring now to Figure 3b, the local decryptor 221 outputs a decrypted bitstream 344 and contains logic similar to the local encryptor 220. For example, it contains an even key register 302b, an odd key register 304b, a hidden register 310b, and key decryption logic 312b. The local decryptor 221 also contains logic 326 suitable to decrypt the bitstream 342 which the local encryptor 220 encrypted. The bitstream decryptor 326 reads the TSC bits in the bitstream 342 and uses that value to determine whether to use the even key or the odd key. For example, switch 325 may be controlled by TSC signal 328. The connection between the hidden register 310b and the communication link 215 is optional. The broadcast decryptor 202 features the same logical circuitry as the local decryptor 221.

Referring now to Figure 4, the steps of a process 400 for encrypting keys before transferring them across a bus (e.g., communication link 215) will be discussed. Process 400 may be implemented as instructions stored in computer memory and executed over a processor of any general purpose computer system. In step 405, an encrypted bitstream is received, for example, by frontend (Figure 2, 201).

In optional step 410, a hidden register 310 is accessed by the host computer system 214. In one embodiment, the developer of the software for host system 214 has knowledge of how to access the hidden register 310; however, the hidden register 310 is otherwise inaccessible so as to minimize theft of the encryption keys and hence the encrypted signal. Conveniently, this hidden register 310c may be within the broadcast decryptor 202, as the key will be sent to that component. However, in other embodiments, the hidden register 310 may be anywhere in first circuit 203.

In one embodiment, the host computer system 214 has knowledge of the value in the hidden register 310; therefore, it does not need to access the hidden register 310. For example, a software engineer provides the host system 214 with the value which was or will be stored into the hidden register 310 at manufacture time. In this embodiment, the hidden register 310 may be inaccessible from outside the circuit, thus providing added security.

In step 415 the broadcast key is determined at a location separate from where the bitstream is to be decrypted. For example, the key may need to be transferred across a communication link 215 to get to the broadcast decryptor 202. To determine the key, key information may be extracted from the bitstream and sent the host computer system 214. The host system 214 communicates with the Smartcard 213 to determine the encryption key. The present invention is well-suited to using other methods for determining the broadcast encryption key. For example, the Smartcard 213 is for illustrative purposes only. This key may be

frequently renewed and may be an odd or an even key, and may be accomplished using well known methods.

In step 420, the host computer system 214 encrypts the broadcast key. The value which is in the hidden register 310c in the first logical circuit 203 is used. Consequently, the first circuit 203 will be able to decrypt the broadcast key using this value, provided the first circuit 203 knows the encryption method used by the host computer system 214. As stated herein, the present invention, provides great flexibility regarding the hidden registers 310, which may be read or written, but do not have to be, in various embodiments.

In step 425, the encrypted broadcast key is transferred across the bus 215 by the host system 214. As the key is encrypted, the conventional art problem of theft is minimized dramatically.

In step 430, the first circuit 203 decrypts the broadcast key. The first circuit 203 has access to the value in the hidden register 310c, which it uses, along with knowledge of the encryption technique, to decrypt the key. For example, in one embodiment an exclusive OR is performed between the value in the hidden register 310c and the encrypted key.

Using this key, the first circuit 203 is now able to decrypt the signal (bitstream), in step 435. The signal may now be sent to the DTCP block 223 so that the signal may be encrypted for transfer across to IEEE 1394 bus and stored

for later play. Alternatively, the signal may be sent directly to the local encryptor 220 such that the signal may be transferred to the second logical circuit 204.

Referring now to Figure 5, the steps of a process 500 for securely transferring a bitstream between circuits will be discussed. Process 500 may be implemented as instructions stored in computer memory and executed over a processor of any general purpose computer system. In step 505, the local encryptor 220 receives the un-encrypted signal from either the broadcast decryptor 202 or the DTCP decryptor 233.

In optional step 510, the hidden registers 310a and 310b are accessed by the host computer system 214. Other embodiments provide the host system 214 with the value in the hidden registers 310 in other fashions, as described herein. In one embodiment, the hidden registers 310a and 310b, respectively, in circuits 220 and 221 contain different values. Furthermore, even if the values from one set-top decoder box are discovered, the security of other boxes in not compromised, because other boxes are manufactured with different values.

In step 515, the local encryption key (odd or even) is generated by the host computer 214. The process 500 cycles from step 515 through step 560 with the host processor 214 alternating between sending out odd and even keys. Additionally, the local encryption key generated in one set-top box system may be different from other set-top boxes. Therefore, even were the local encryption key to be stolen, it would do no good to pass it to another set-top box. This is in

contrast to some conventional systems for which all set-top boxes use the same encryption key, at least for a period of time.

In step 520, the local key is encrypted for the first 203 and the second 204 circuits. In a preferred embodiment, an Exclusive OR is performed between the value from a hidden register 310 and the local key. Because the first and second circuits may have their own hidden register 310 values, the encryption will be different for each circuit.

In step 525, the encrypted keys are transferred across the bus 215 to the first 203 and the second 204 circuits. A 64-bit value in the hidden register 310 will provide 2^{64} possible combinations. Therefore, it will be very difficult to obtain the original key from the encrypted (XORed) key without the secret hidden value.

In step 530, the host computer 214 sends a command to the first circuit 203 to modify the TSC bits in the header of the bitstream to indicate that the bitstream is encrypted. Additionally, the command may indicate the type of encryption key, for example, odd or even. The circuit 203 then modifies the header to indicate the type of encryption key.

In step 535, the local key is decrypted at the first circuit 203 using the value from the hidden register 310a. In step 540, the second encrypted local key is decrypted at the second logical circuit 204. The odd and even key registers (304b, 302b) allow the host computer 214 to send the ever changing keys out somewhat ahead of the time the bitstream requires a new key for decryption.

Then, in step 545, the bitstream is encrypted, for example by bitstream encryption logic 306. Any convenient encryption method may be used here, for example, data encryption standard (DES) may be used.

In step 550, the TSC bits are modified in the bitstream header. In this fashion, the local decryptor 221 will be able to determine necessary information to decrypt the locally encrypted bitstream 342, for example, whether the key is odd or even. This facilitates key switching which makes theft of the bitstream more difficult.

In step 555, the bitstream is transferred from the first integrated circuit 203 to the second integrated circuit 204. Unlike some conventional systems, the bitstream is encrypted for protection, in this embodiment.

In step 560, the local decryptor 221 uses the local encryption key to decrypt the signal it received from the local encryptor 220. In step 565, the decrypted bitstream 344 is sent on to the transport parser/de-multiplexer 207 and so on for decoding.

For added security, an embodiment illustrated in Figure 7 contains multiple hidden registers. While the local encryptor 220 is shown, this embodiment is equally suited to the decryptors (202, 221). At least one hidden register 310 is selected for use, for example, by the host computer system 214. The selected hidden register(s) 310 may be indicated to the first and second circuits (203, 204)

via a bit or bits which are set in a control register 315. For example, in one embodiment, the host processor 214 may use the value in either a first hidden register 310 or a second hidden register 310 or both hidden registers 310 in the encryption process. Any suitable method may be used to indicate which hidden register(s) 310 are used. For example, a value of "01" for a first hidden register, "10" for a second hidden register, and "11" for both is sent from the host 214 to the control register 315. The present invention is well-suited to using any number of hidden registers 310. Furthermore, the host 214 may periodically change the value in the control register 315 (along with the key encryption).

Referring to Figure 8, in yet another embodiment, rather then using a hidden register 310, user-dependent data may be used to derive local encryption keys. For example, the digital bitstream decryptor and decoder 200 has non-volatile memory 317 to store user-dependent data, such as favorite TV programs, pay-per-view charges, etc. The host computer system 214 accesses this non-volatile memory 317 to generate a unique key for each set-top box (e.g., digital bitstream decryptor and decoder 200).

For still more secure key encryption other bit operations such as bit-inversion, bit-shift, bit-permutation, or the like may be applied. In one embodiment, these operations are combined. Furthermore, the combinations used may be varied. In these embodiments, the host processor 214 will indicate to the circuits (203, 204) which encryption method is currently being used.

Another embodiment provides for a method of detecting possible tampering with the system. In this method, the host computer 214 periodically polls all the related hidden registers 310 in broadcast decryptor 202, local encryptor 220, and local decryptor 221. If a discrepancy is detected, host computer system 214 goes into emergency mode and shuts down the whole system. Furthermore, host computer system 214 may send out an alert to the broadcast service provider indicating the possible tampering. This embodiment, makes it difficult for a hacker to illegally modify the values in the hidden registers 310.

Figure 6 illustrates circuitry of computer system 100, which may form a platform for a portion of the host computer system 214, the broadcast decryptor 203, the local encryptor 220, or the local decryptor 221. Computer system 100 includes an address/data bus 99 for communicating information, a central processor 101 coupled with the bus for processing information and instructions, a volatile memory 102 (e.g., random access memory RAM) coupled with the bus 99 for storing information and instructions for the central processor 101 and a non-volatile memory 103 (e.g., read only memory ROM) coupled with the bus 99 for storing static information and instructions for the processor 101. Computer system 100 also includes an optional data storage device 104 coupled with the bus 99 for storing information and instructions.

Also included in computer system 100 of Figure 6 is an optional alphanumeric input device 106. Device 106 can communicate information and command selections to the central processor 101. System 100 also includes an optional cursor control or directing device 107 coupled to the bus 99 for

communicating user input information and command selections to the central processor 101. The display device 105 utilized with the computer system 100 may be a liquid crystal device, cathode ray tube (CRT), field emission device (FED, also called flat panel CRT) or other display device suitable for creating graphic images and alphanumeric characters recognizable to the user. Signal input/output communication device 108 is also coupled to bus 99.

The preferred embodiment of the present invention a method and system for securely decrypting and decoding a digital signal is thus described. While the present invention has been described in particular embodiments, it should be appreciated that the present invention should not be construed as limited by such embodiments, but rather construed according to the below claims.

CLAIMS

What is claimed is:

1. A method of processing a digital signal comprising the steps of:

a) receiving an encrypted signal at a first logical circuit;

b) determining a broadcast encryption key for said encrypted signal at a first location separate from said first logical circuit;

c) encrypting said broadcast encryption key;

d) transferring said encrypted broadcast encryption key over a communication link;

e) at said first logical circuit, decrypting said encrypted broadcast encryption key to determine said broadcast encryption key; and

f) at said first logical circuit, decrypting said encrypted signal using said broadcast encryption key.

2. The method of Claim 1 wherein said step c) comprises the steps of:

c1) accessing a value in a hidden register on said first logical circuit; and

c2) using said value accessed in said step c1), encrypting said broadcast encryption key.

3. The method of Claim 2 wherein said step c) further comprises the step of:

c3) modifying the value in said hidden register.

4. The method of Claim 1 further comprising the steps of:

g) storing a value in a hidden register on said first logical circuit; and

h) providing said value to a host computer system to use for encryption.

5. The method of Claim 1 wherein said step e) further comprises the steps of:

e1) accessing a value in a hidden register on said first logical circuit; and

e2) using said value accessed in said step e1), decrypting said encrypted broadcast encryption key.

6. The method of Claim 1 wherein said received bitstream is substantially compliant the with Motion Pictures Experts Group (MPEG) format.

7. The method of Claim 1 wherein said step c) further comprises the steps of:

c1) selecting at least one of a plurality of hidden registers on said first logical circuit to be used to encrypt said broadcast encryption key; and

c2) indicating said selection to said first logical circuit.

8. The method of Claim 1 wherein said step c) comprises the steps of:

c1) accessing a value in non-volatile memory on said first logical circuit; and

c2) using said value accessed in said step c1), encrypting said broadcast encryption key.

9. The method of Claim 8 wherein said non-volatile memory contains user-dependent data.

10. A method of processing a digital signal comprising the steps of:

a) generating a local encryption key;

b) transferring said local encryption key across a communication link to a first logical circuit and to a second logical circuit;

c) with said local encryption key, encrypting said digital signal at said first logical circuit;

d) transferring said digital signal to said second logical circuit; and

e) using said local encryption key, decrypting said digital signal at said second logical circuit, wherein said digital signal is transferred from said first logical circuit to said second logical circuit in an encrypted form.

11. The method of Claim 10 further comprising the step of:

f) before transferring said local encryption key across said communication link, encrypting said local encryption key.

12. The method of Claim 11 wherein said step f) comprises the steps of:

f1) accessing a value in a register in said first logical circuit; and

f2) based upon said value accessed in said step f1), encrypting said local encryption key.

13. The method of Claim 11 wherein said step f) comprises the steps of:

f1) accessing a value stored in a register in said second circuit; and

f2) based upon said value accessed in said step f1), encrypting said local encryption key.

14. The method of Claim 10 further comprising the step of:

f) issuing a command to said first logical circuit to modify a header in said bitstream to indicate that said bitstream is encrypted.

15. The method of Claim 14 wherein the command further indicates the type of encryption wherein said type is between even and odd.

16. The method of Claim 10 further comprising the step of:

f) switching said local encryption key between odd and even encryption.

17. The method of Claim 10 further comprising the steps of:

f) polling a first hidden register in said first logical circuit;

g) determining whether the value in said hidden register has been modified; and

h) stopping said processing of said digital signal if said register has been modified.

18. The method of Claim 17 further comprising the step of:

i) sending a message to a broadcast provider if said step j) determined that said hidden register was modified.

19. A system for processing a digital signal, comprising:

a first logical circuit comprising a first hidden register and a local encryptor, said first logical circuit operable to decrypt a first local key using a first value stored in said first register; and

a second logical circuit comprising a local decryptor and a second hidden register, said second logical circuit operable to decrypt a second local key using a second value stored in said second register, said local decryptor operable to decrypt a signal encrypted with said local encryptor.

20. The system of Claim 19 further comprising:

a host processor;

a communication link connecting said host processor to said first logical circuit and to said second logical circuit; and

memory coupled to said host processor, said memory containing instructions which when run on said host processor are operable generate said first local key and to generate said second local key.

21. The system of Claim 20 wherein said memory further comprises instructions operable to access said first hidden register.

22. The system of Claim 19 wherein said first logical circuit further comprises:

a 1394 encryptor operable to encrypt a signal for transfer over an IEEE 1394 communication link.

23. The system of Claim 19 wherein said first logical circuit further comprises:

a broadcast decryptor comprising a broadcast hidden register, said broadcast decryptor operable to decrypt a broadcast signal and to decrypt an encrypted key using a value in said broadcast hidden register.

24. The system of Claim 22 wherein said memory further contains instructions which when run on said host processor are operable to generate a broadcast encryption key, to access said broadcast hidden register, and to encrypt said broadcast encryption key.

25. The system of Claim 19 wherein said first logical circuit further comprises a plurality of hidden registers and a control register operable to store a value to indicate which of said hidden registers is used for encryption.

METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER

ABSTRACT

A method and system for securely decrypting and decoding a digital signal. One embodiment of the present invention first receives an encrypted signal at a first logical circuit. Next, this embodiment determines a broadcast encryption key for the encrypted signal at a first location separate from the first logical circuit. For example, the separate location where the broadcast key was determined may be across a communication link from the first circuit where the signal is being received. Then, the broadcast encryption key is encrypted and transferred over the communication link. Next, at the first logical circuit, the encrypted broadcast encryption key is decrypted. Therefore, the broadcast encryption key is determined. Then, at said first logical circuit, the encrypted signal is decrypted using the broadcast encryption key. Consequently, the encrypted signal is decrypted without exposing the broadcast encryption key on the communication link in an un-encrypted form. Another embodiment provides a method which first generates a local encryption key. Then, the local encryption key is transferred across a communication link to a first logical circuit and to a second logical circuit. With the local encryption key, a digital signal at the first logical circuit is encrypted. This encrypted signal is transferred to the second logical circuit. Thus, the signal is not exposed in an un-encrypted form. Next, the second logical circuit uses the local encryption key to decrypt the signal.

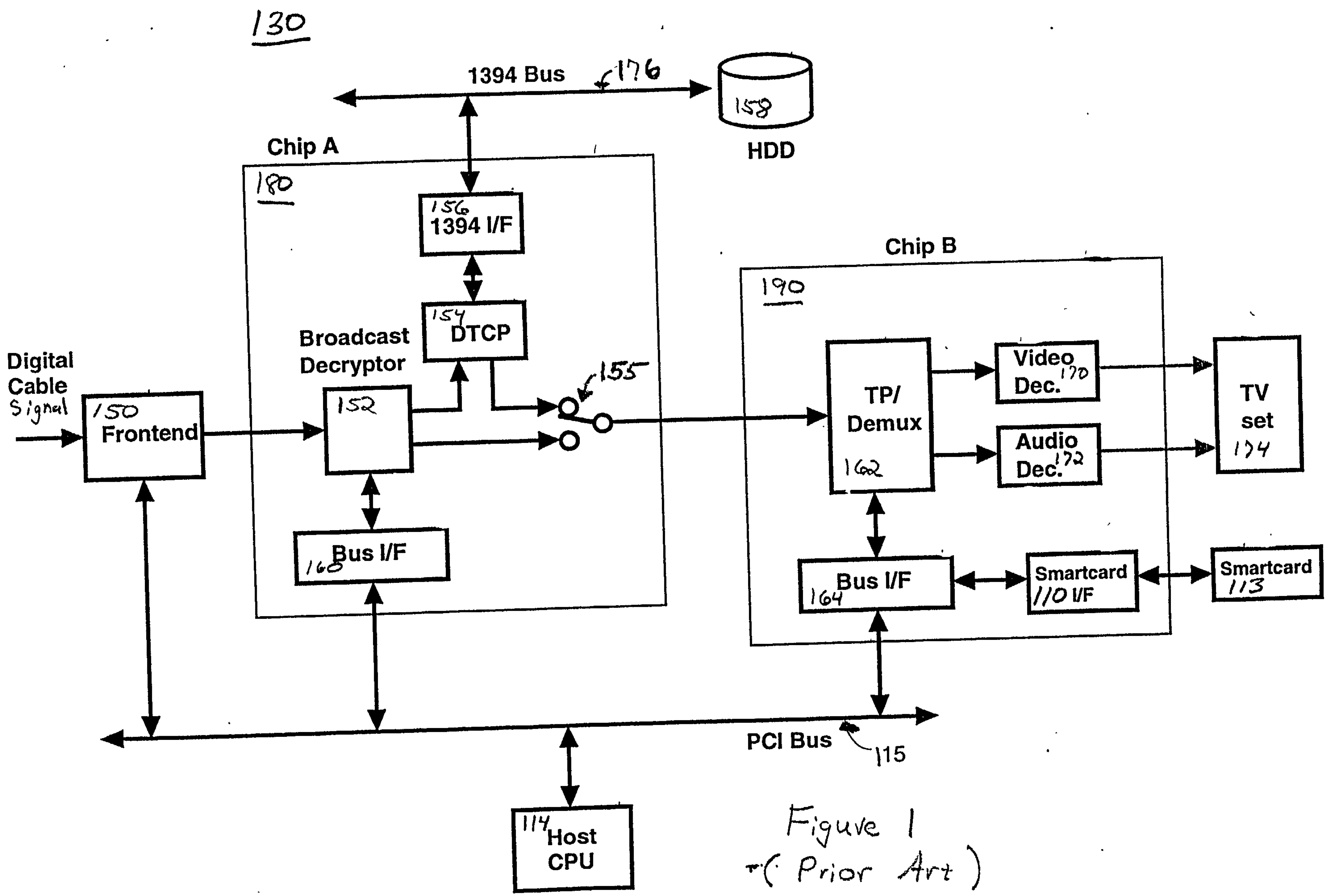

Figure 1
(Prior Art)

00420T"48596960

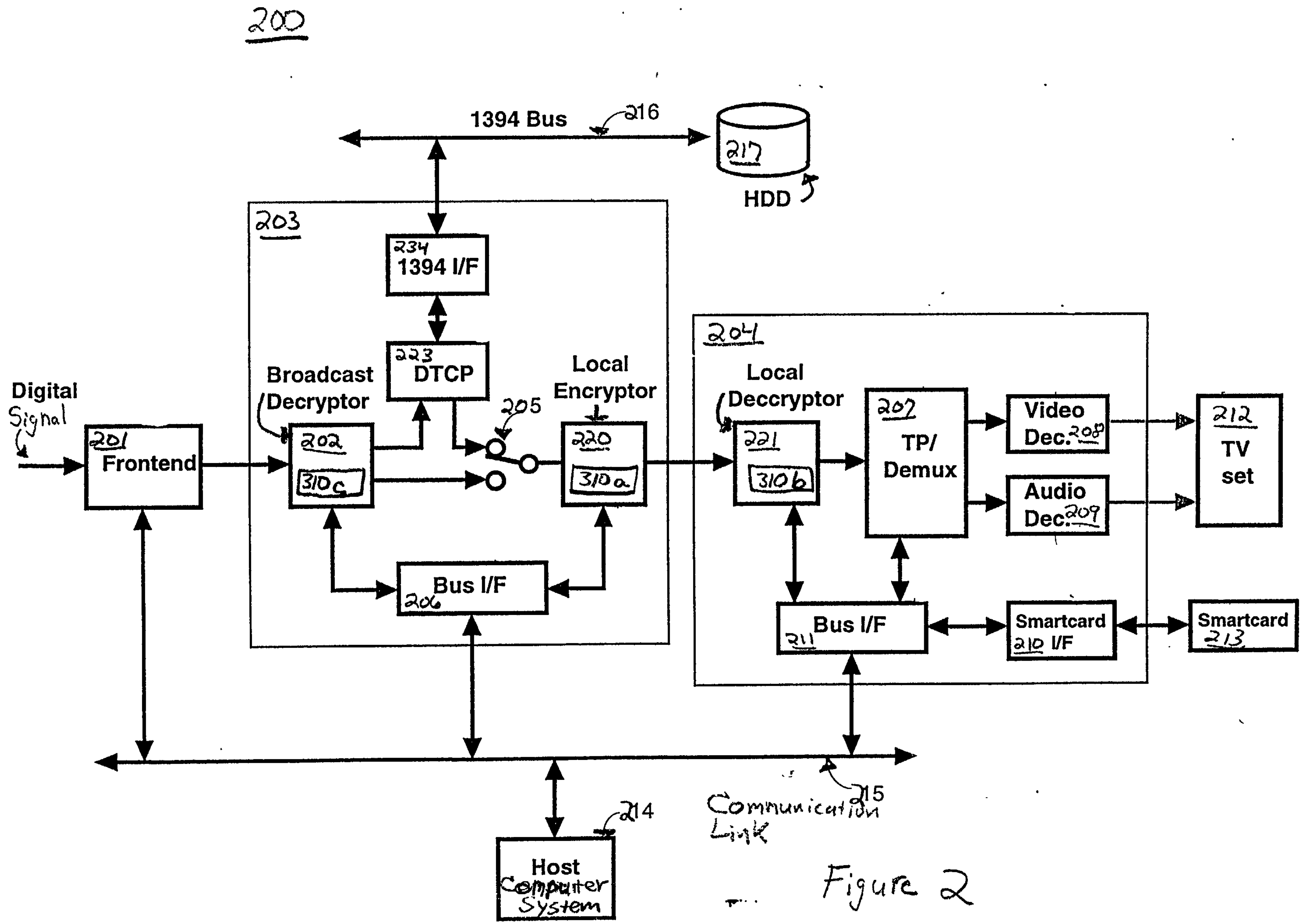

Figure 2

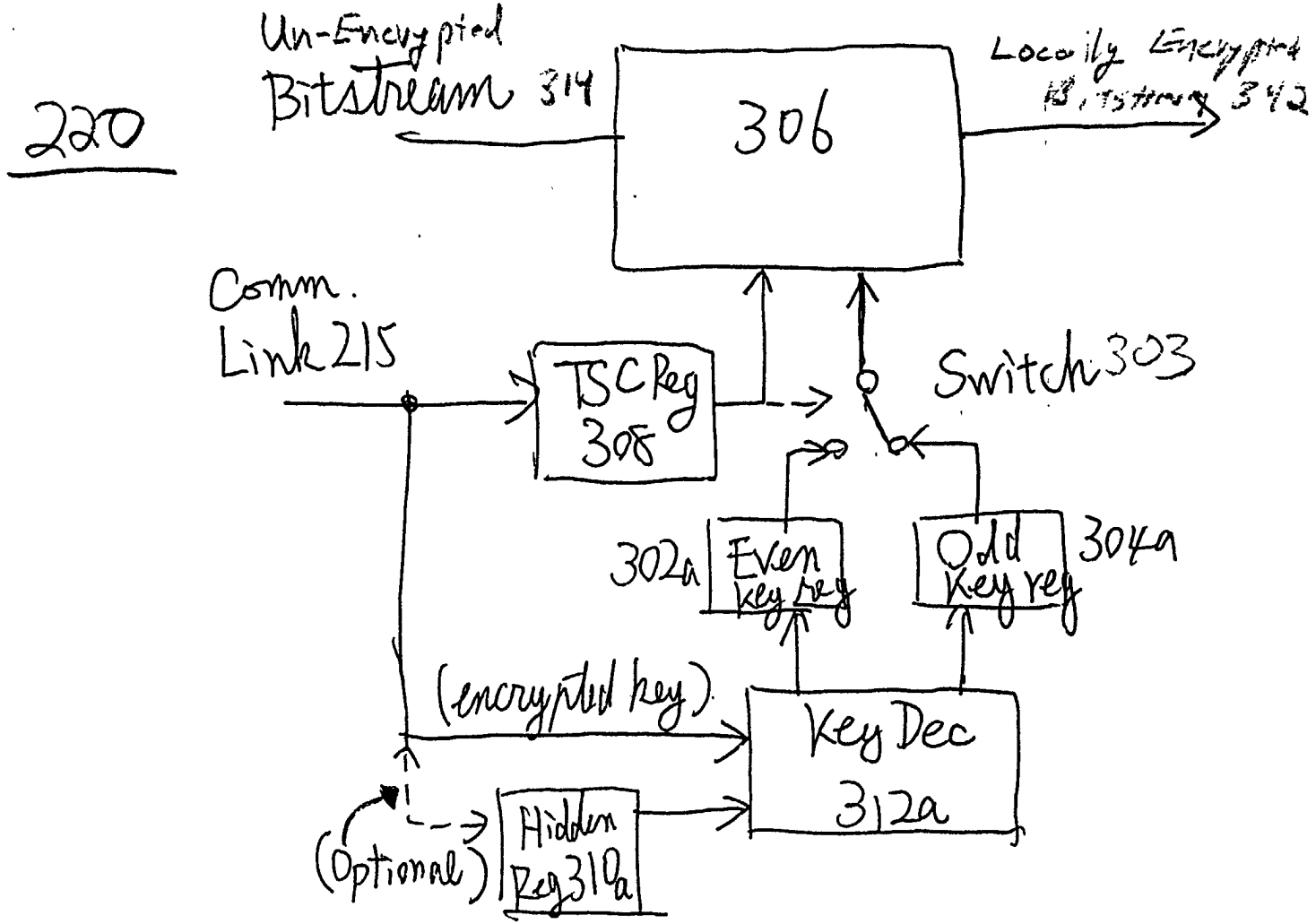

Figure 3A. Local Encryptor

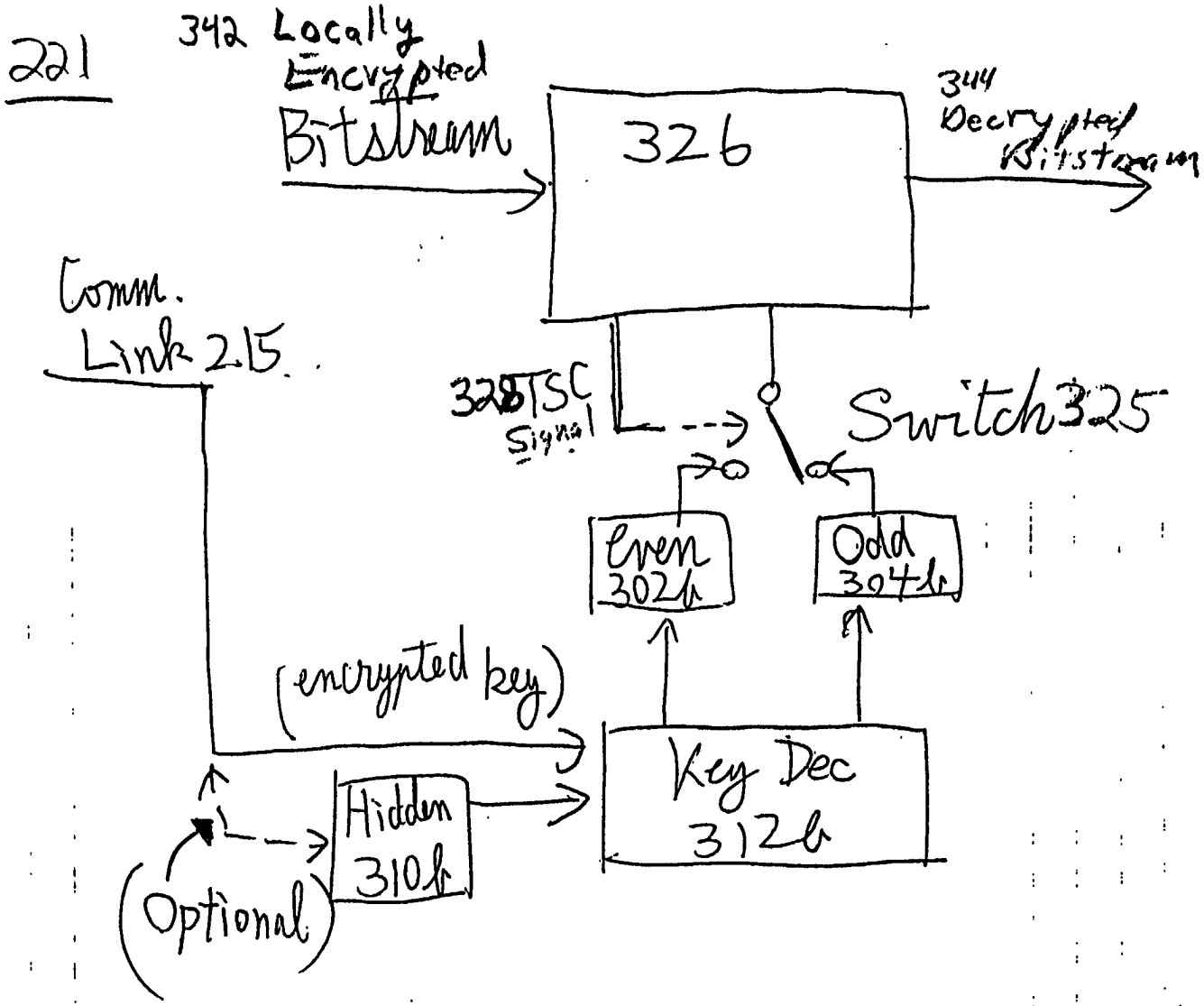

Figure 3B. Local Decryptor

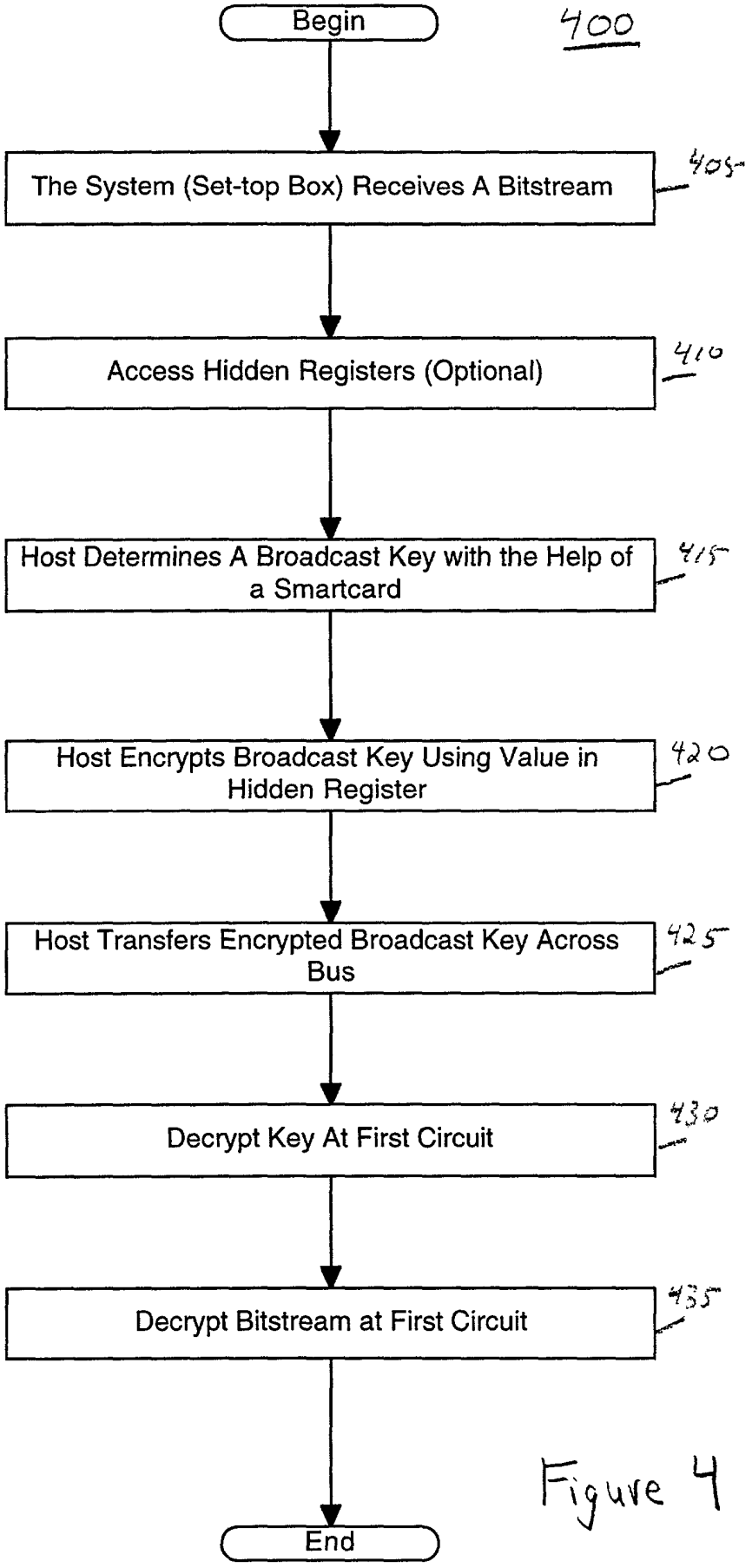
Begin
400
The System (Set-top Box) Receives A Bitstream
405
Access Hidden Registers (Optional)
410
Host Determines A Broadcast Key with the Help of a Smartcard
415
Host Encrypts Broadcast Key Using Value in Hidden Register
420
Host Transfers Encrypted Broadcast Key Across Bus
425
Decrypt Key At First Circuit
430
Decrypt Bitstream at First Circuit
435
End

Figure 4

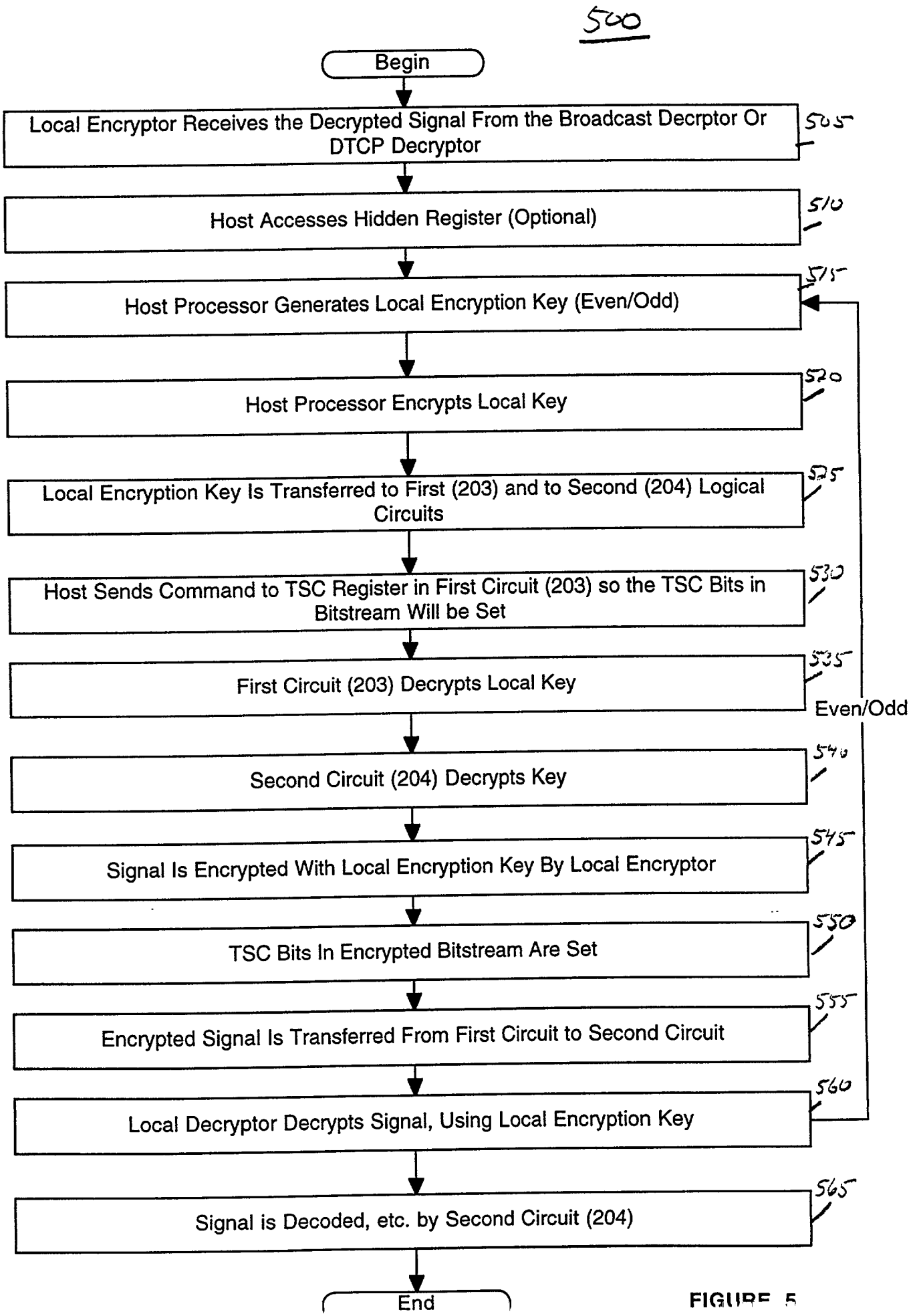
500
Begin
Local Encryptor Receives the Decrypted Signal From the Broadcast Decrptor Or DTCP Decryptor
505
Host Accesses Hidden Register (Optional)
510
Host Processor Generates Local Encryption Key (Even/Odd)
515
Host Processor Encrypts Local Key
520
Local Encryption Key Is Transferred to First (203) and to Second (204) Logical Circuits
525
Host Sends Command to TSC Register in First Circuit (203) so the TSC Bits in Bitstream Will be Set
530
First Circuit (203) Decrypts Local Key
535
Second Circuit (204) Decrypts Key
540
Signal Is Encrypted With Local Encryption Key By Local Encryptor
545
TSC Bits In Encrypted Bitstream Are Set
550
Encrypted Signal Is Transferred From First Circuit to Second Circuit
555
Local Decryptor Decrypts Signal, Using Local Encryption Key
560
Signal is Decoded, etc. by Second Circuit (204)
565
End
Even/Odd

FIGURE 5

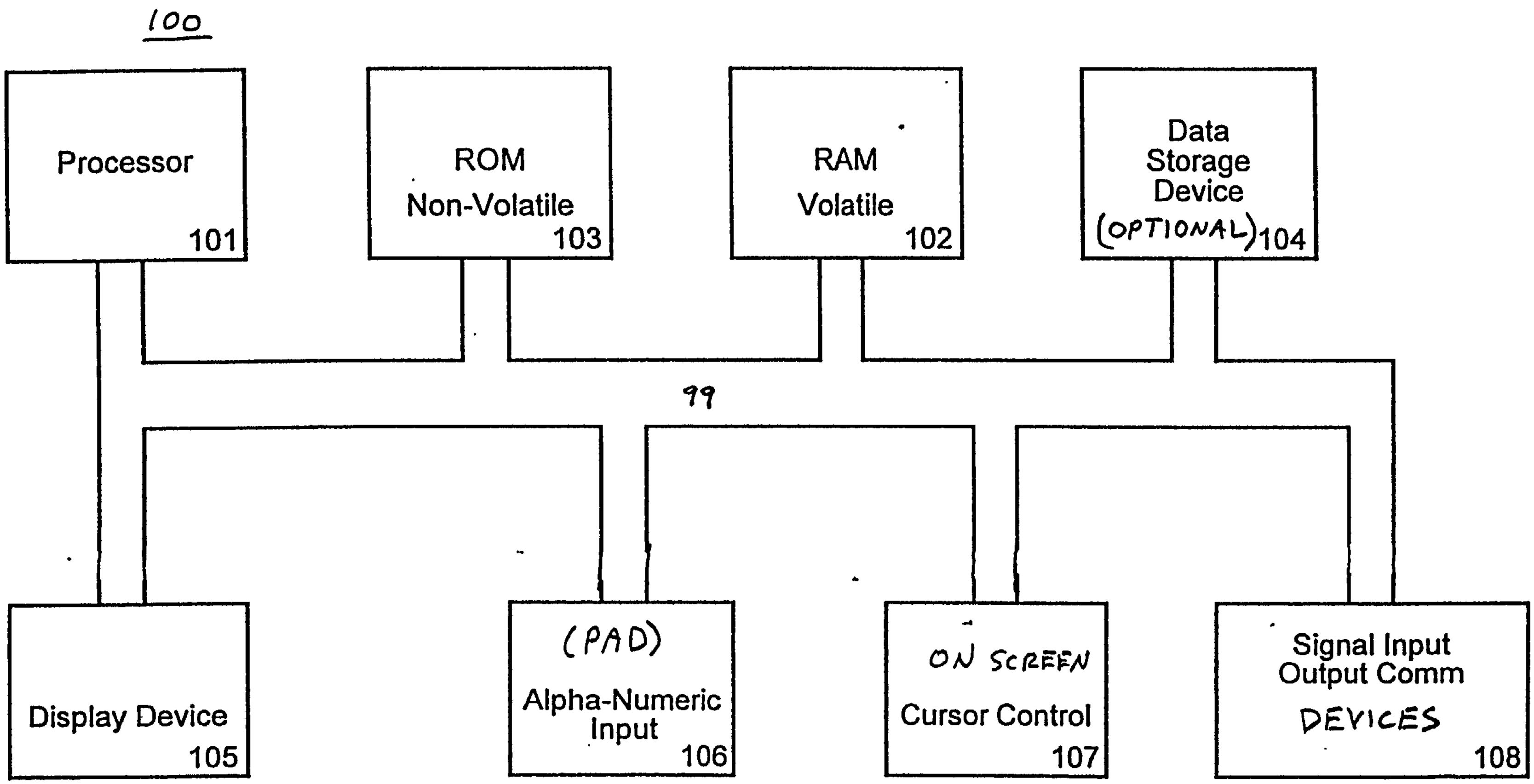

FIG. 6

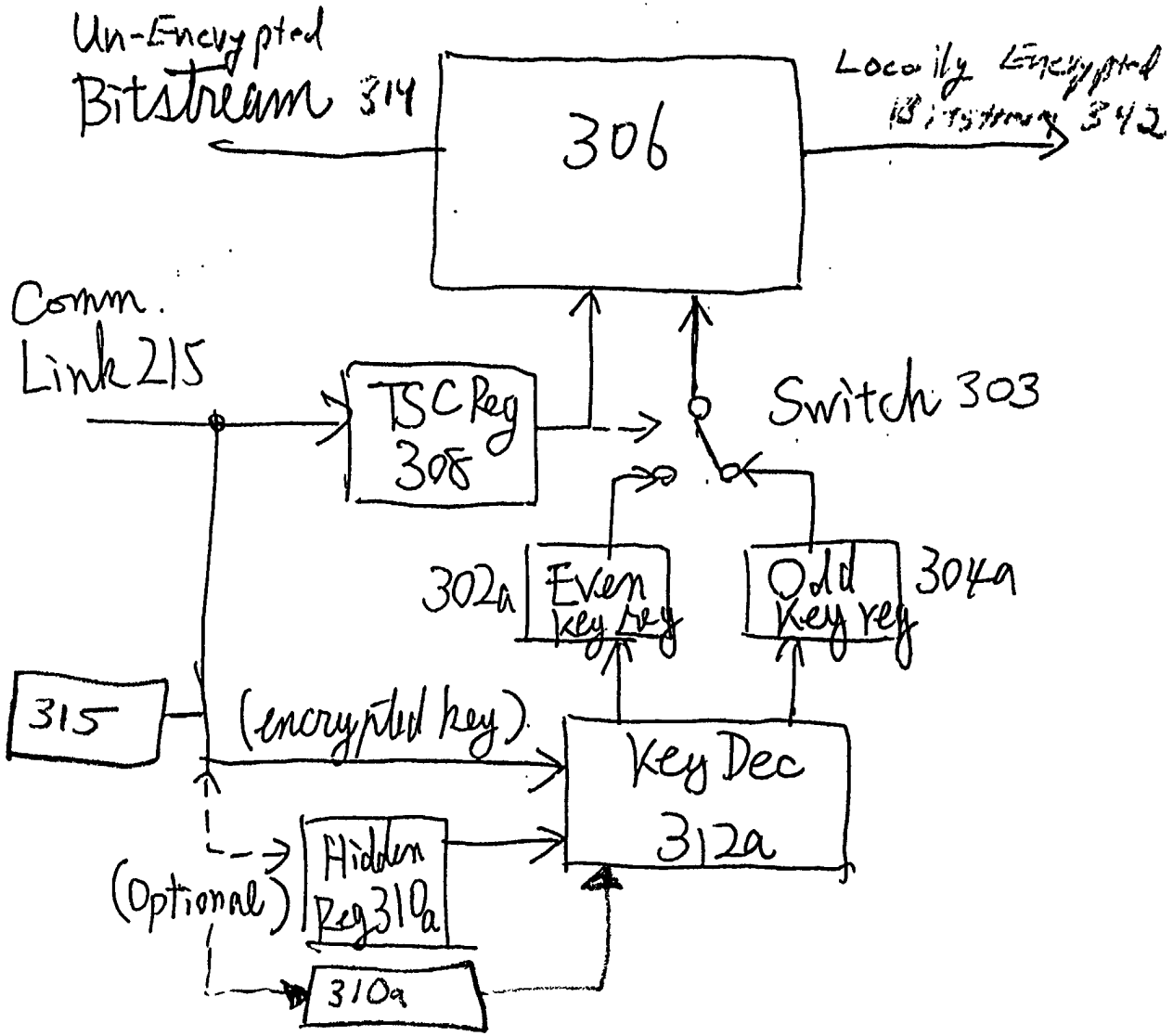

Figure 7

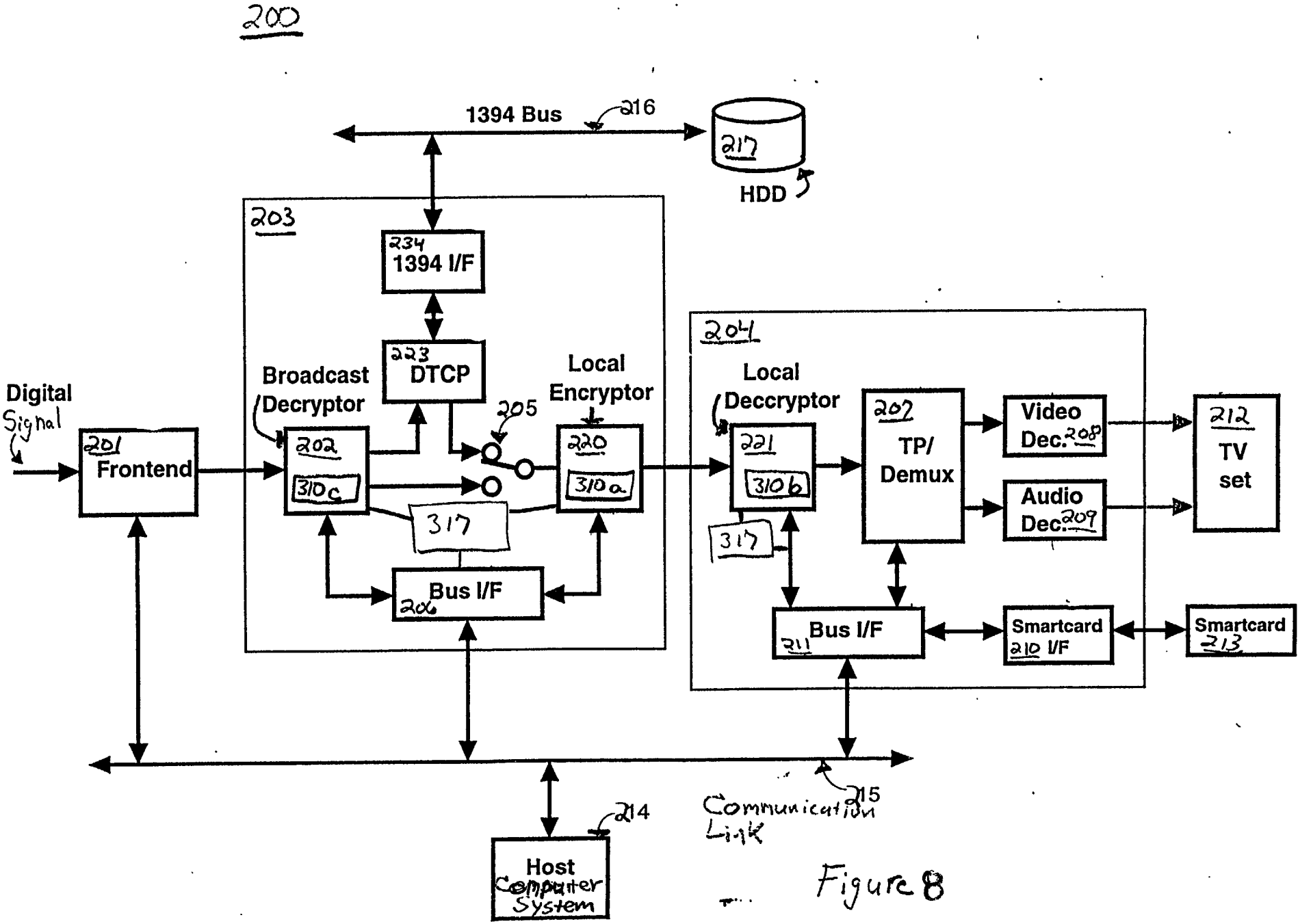
200
1394 Bus
216
217
HDD
203
234
1394 I/F
223
DTCP
Broadcast
Decryptor
Local
Encryptor
205
Digital
Signal
201
Frontend
202
310c
220
310a
317
Bus I/F
206
204
Local
Deccryptor
221
310b
317
202
TP/
Demux
Video
Dec.208
Audio
Dec.209
212
TV
set
Bus I/F
211
Smartcard
210 I/F
Smartcard
213
215
Communication
Link
214
Host
Computer
System

Figure 8

Declaration and Power of Attorney for a Patent Application

Declaration

As below named inventor, I hereby declare that my residence post office address, and citizenship are as stated below my name. Further, I hereby declare that I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND SYSTEM FOR A SECURE DIGITAL DECODER

the specification of which:

X is attached hereto, or
_____ was filed on _____ as application serial no. _____ : and
_____ was amended on _____

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above; and

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

Foreign Priority Claim

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Number	Country	Date Filed	Priority Claimed	
			yes	no
			yes	no

U.S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 and 199(e) of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Serial Number	Filing Date	Status (patented/pending/abandoned)

Power of Attorney

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent Trademark Office connected therewith.

James P. Hao	Registration No.: 36,398
Anthony C. Murabito	Registration No.: 35,295
John P. Wagner	Registration No.: 35,398
Glenn D. Barnes	Registration No.: 42,293
Rick G. Brewster	Registration No.: 35,077
Thomas M. Catale	Registration No.: 46,434
Jose S. Garcia	Registration No.: 43,628
Kenneth N. Glass	Registration No.: 42,587
Lin C. Hsu	Registration No.: 46,315
Patrick W. Ma	Registration No.: 44,215
Ronald M. Pomerenke	Registration No.: 43,009
John F. Ryan	Registration No.: 47,050
William A. Zarbis	Registration No.: 46,120
Matthew J. Blecher	Registration No.: 46,558

Send Correspondence to:

WAGNER, MURABITO & HAO LLP
Two North Market Street
Third Floor
San Jose, California 95113
(408) 938-9060

Signatures

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor: **Ryuichi Iwamura**

Inventor's Signature × [signature] Date × October 19, 2000

Residence San Diego, CA Citizenship Japan
(City State)

P.O. Address 11864 Paseo Lucido, #2083, San Diego, CA 92127

rev. 2/00 kgr